Testimony of Daniel Galik
Chief, Mission Assurance and Security Services
Internal Revenue Service
Before the
House Committee on Government Reform
June 8, 2006

Good morning Chairman Davis, ranking Member Waxman and members of the Committee on Government Reform. My name is Dan Galik. I am the Chief of Mission Assurance and Security Services (MA&SS), and serve as the Chief Security Officer for the Internal Revenue Service. I am pleased to be with you this morning to discuss IRS's efforts relative to information technology (IT) security and the privacy of both employee and taxpayer information.

Taxpayer and employee privacy is a foremost concern of the IRS. We are charged with protecting the most critical information about virtually every American. In recognition of this responsibility, we continue to update our systems and our training so that employees who have access to sensitive information are aware of the steps they must take to prevent that information from being compromised.

This job has never been tougher. According to the FBI, identity theft is one of the fastest growing White Collar crimes. There has been a 4,600 percent increase in computer crime since 1997. Nearly 20 million Americans lost their identities over the past two years, according to the Federal Trade Commission. Deloitte-Touche recently reported that financial institutions and U.S. banks have also experienced a significant increase in the number of computer based attacks and attempted intrusions into financial systems.

Contrast that with the job of the IRS. Every year, we process approximately $2 trillion in revenues to fund the U.S. operating budget. Although the majority of this is collected in an automated banking system throughout the year, about $300 billion is collected through 8 IRS campuses where taxpayers send their tax returns for processing. We house computing systems that hold data on all taxpayers and also process enormous volumes of paper data in our more than 500 offices across the country. We have more than 82,000 full time and 12,000 part-time employees across the U.S.

As a result, protecting all of this information has simultaneously become both more important and more difficult. Imagine if you will a chain with each link representing some element of information security such as security policies and processes, training, or the use of encryption mechanisms. It is a cliché to say we are no stronger than our weakest link, but it is true. Those seeking to unlawfully access this data have the ability to attack our weakest link. Perhaps the strongest asset that IRS deploys in trying to counter information security breaches is our layered "defense in depth" concept. In short, attackers must defeat multiple security protection layers to get to our data.

I would be disingenuous if I did not say that what happened at the Department of Veterans Affairs (VA) has probably caused everyone in my position in the Federal government to take a second look at all of the policies and procedures in place to prevent a similar incident for our agency. And, regardless of how rigorous our programs or how much training we conduct, it can still happen.

We recently had an incident at the IRS where an employee, heading to a job fair, checked a carrying case as luggage on a commercial flight. The carrying case contained a laptop computer and an accompanying finger print scanner. The laptop contained the fingerprints and some personal data on 291 IRS employees and job applicants. The information contained on the laptop was limited to information job applicants provide and included the name, date of birth, social security number, and physical characteristics of the applicant (height, weight, hair color, etc.). There were no electronic tax records or financial information on the laptop. The laptop was lost in transit and has not been recovered.

According to our procedures, this was reported to the Treasury Inspector General for Tax Administration (TIGTA), which is currently conducting an investigation. The airlines and other federal officials are also investigating. In addition, we contacted each of the individuals whose information was on the laptop by phone and by letter to inform them of the missing data and to guide them on how to watch for suspicious activity. We are now reviewing and refining our procedures for handling fingerprint equipment to reduce the possibility of this happening in the near future. We are also working with the provider of the fingerprint equipment in installing encryption capabilities. Later in my testimony, I will discuss the encryption procedures we plan to implement for laptops. This morning, I want to describe to you the steps we have taken and are taking to protect sensitive data. First, however, I think it is important for you to better understand the security environment in which the IRS operates.

Mission Assurance and Security Services

Under the IRS Restructuring and Organization Act of 1998 (RRA), our agency was essentially divided into two distinct units. One unit focuses on service and enforcement and represents the primary point of contact between the IRS and all taxpayers. The other unit focuses on operations support for the agency. In essence, the Operations Support unit, of which MA&SS is a part, provides the tools for the Services and Enforcement division to do its job. As the chief of MA&SS, I report directly to the Deputy Commissioner for Operations Support.

MA&SS is a service and support organization. It assists all IRS Operating Divisions in maintaining secure facilities, technology, and data. We provide the operational support to enable an integrated approach to information protection by combining physical, information technology, and personnel security as well as privacy. We do so by providing overall IRS security and privacy leadership and promoting collaborative security planning and decision-making with all IRS organizations.

MA&SS brings together previously separate security functions to enable a consistent and unified approach to security and privacy. The MA&SS organization is matrixed to enable an integrated approach to meeting security needs. Five core programs – Information Technology Security, Physical Security, Emergency Preparedness, Personnel Security, and Privacy – shape the direction of services and initiatives.

For the purposes of this hearing, I will focus my attention on two of these programs: Information Technology (IT) and Personal Security and Privacy.

Information Technology Security

Our Information Technology Security Program Office is charged with identifying and mitigating threats, establishing policy and standards, determining strategy and priorities, and monitoring program implementation. In addition, the office provides customers with the tools, advice, security engineering, and tactical guidance necessary to ensure IT security is properly addressed in the development and operations of all IRS information systems.

Title III of the E-Government Act, entitled Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information systems that support the operations and the assets of the agency. As required by FISMA, the IRS has implemented an agency-wide information technology security program which includes following key elements:

- Periodic assessments of risk;
- Policies and procedures that are based on risk assessments;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems as appropriate;
- Security awareness training to inform personnel (including contractors) of the information security risks associated with their activities and their responsibilities in complying with IRS policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices and security controls;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures and practices of the IRS;
- Procedures for detecting, reporting and responding to security incidents; and

- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets.

The IRS IT Security Program efforts in 2004 and 2005 were focused on the accomplishment of security certification and accreditation of the IRS network infrastructure systems, which was achieved at the end of FY 2005. The top priority in FY 2006 has been on achieving security certification and accreditation for our major applications, using new process guidance issued each year by the National Institute of Standards and Technology (NIST). As a result, over 90 percent of our major systems having successfully completed security certification and accreditation. (Of note, in early 2004, very few of the IRS' major information systems had completed security accreditation). The IRS will continue to aggressively pursue the correction of the computer security material weaknesses and implementation of the corrective plans that address those weaknesses. The IRS is implementing an enterprise-wide risk management approach that cost-effectively focuses resources on major systems and assets that directly support the most critical business processes supporting tax administration. While we have made significant progress towards implementation of a FISMA compliant IT Security program at the IRS, we anticipate that progress continuing in 2006 and 2007 as we transition to high quality certification and accreditation packages for all IRS systems. With the increased recent attention on privacy and identity theft, the IRS is ensuring that proper management, operational, and technical security and privacy controls are enhanced for existing legacy infrastructure systems, and also built into the designs for all new tax modernization systems.

The day-to-day security status of the entire IRS network and computer operations are continuously monitored by a world class 24X7 Computer Security Incident Response Center (CSIRC). The IRS CSIRC provides proactive prevention, detection, and response to computer security incidents targeting the IRS' enterprise IT assets. The CSIRC is equipped to identify, contain and eradicate cyber threats targeting IRS computing assets. The four major CSIRC operational functions of prevention, detection, response and reporting meet FISMA requirements for incident response and reporting. IRS IT security technical efforts have focused on "hardening" computer and network infrastructure systems to make them resistant to external attacks. We believe there have been no successful penetrations into any IRS systems by hackers. The IRS has deployed the security "defense-in-depth" approach with over 100 firewalls and several hundred intrusion detection devices, with all of these devices monitored by the CSIRC. Anti-virus software is deployed throughout the network, and the latest security patches and required updates are aggressively pushed out to all desktops.

All IRS computers are equipped with multiple data protection tools that allow all IRS users to encrypt all taxpayer data, personally identifiable information, and all other sensitive information. In light of the incident at the VA, the IRS is aggressively reviewing all policies, processes, and training to ensure IRS users know how to use the encryption tools, are familiar with the associated data protection and privacy policies, and are aware of the penalties for violation of the policies. The primary focus right now is on the large IRS mobile workforce that utilizes laptops and other portable storage devices

working at locations outside of IRS office space. Currently available encryption tools on all IRS computers provide the capability for at least double encryption, and double password protection. The IRS also has the capability to encrypt all sensitive emails. This ultimately provides triple encryption capability and triple password protection for users who utilize both secure email and the other available encryption solutions that are installed on IRS computers. The use of multiple security protection mechanisms enables the IRS to focus increased attention on our internal security controls, to prevent any potential compromises that could occur from an attack by an "insider." The use of the multiple encryption capabilities also prevents or effectively mitigates the loss of any sensitive data, should the user's laptop be stolen, lost, or misplaced. It is important to note that IRS revenue agents in the field utilize software programs that automatically encrypt taxpayer data on the hard drives of their laptops.

The IRS is pursuing the deployment of an enterprise-wide automated security encryption solution for use by all IRS staff. By automatically encrypting all user data files, it removes the challenges faced by typical computer users who may often forget to encrypt sensitive data, or who may not realize that the data they are working with is in fact sensitive. With all taxpayer data files and files that may contain sensitive and personally identifiable information all being encrypted, the IRS will be in a position to mitigate any threats posed by insiders.

The IRS also utilizes a number of software programs that monitor and audit the behavior of the authorized users of IRS tax processing systems. The Integrated Data Retrieval System (IDRS), the System Audit Analysis System (SAAS), and the IRS Internet Misuse and Monitoring Program, all monitor the activities of our users with specific focus on any unauthorized activities, such as attempts to improperly access any taxpayer data.

Office of Privacy and Information Protection

The mission of the Office of Privacy and Information Protection (OP&IP) focuses on enabling taxpayer and employee confidence by ensuring the right people, see the right data, in the right places, for the right reasons. OP&IP achieves this mission by incorporating taxpayer and employee privacy controls and privacy principles of Notice, Choice, Access, Business Purpose, and Data Minimization into IRS systems and business processes. These principles can be generally summarized as "*any information collected about an individual should be the minimum necessary to complete the business at hand and individuals should have access to and notification and choice of the use to which their information is put in order to prevent data inaccuracy and misuse*." This office also ensures that the public is aware of IRS privacy business practices and that IRS programs and projects only gather the taxpayer and employee data necessary to accomplish the Service's objectives. It creates, promotes, and supports privacy awareness Servicewide. The IRS OP&IP begins where the law leaves off, by going the extra step to protect privacy by embedding privacy into IRS systems and business processes and establishing privacy as an agency core value.

Within OP&IP there are a number of subordinate organizations, the IRS Privacy Program the UNAX Program, the Safeguards Program, and the Homeland Security Presidential Directive-12 (HSPD-12) Program Management Office. Today, I will speak on the Privacy, UNAX, and the Safeguards Programs.

The Privacy Program ensures the legal and regulatory privacy requirements are not only met, but exceeded by operationalizing privacy principles through policy, assurance, and awareness programs. The IRS created the Privacy Impact Assessment (PIA) in the early 1990's as a means of identifying privacy risks and vulnerabilities imbedded in IRS systems. The PIA process was identified by the Federal Chief Information Officer Council as a best practice and adopted into law as part of the e-Gov Act of 2002 as the government-wide standard on how to ensure privacy controls throughout the business lines. Specifically, the PIA:

- Ensures handling of personally identifiable information (PII) conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- Determines the risks and effects of collecting, maintaining and disseminating PII in an electronic information system; and
- Examines and evaluates protections and alternative processes for handling PII to mitigate potential privacy risks

We integrate the multiple privacy and confidentiality requirements of the Privacy Act, the e-Gov Act, and Internal Revenue Code into a single program area to increase taxpayer and employee confidence in the way IRS handles personal information.

The OP&IP has expanded its scope to include the Unauthorized Access (UNAX) Program. The mission of the UNAX Program is to provide awareness to all IRS employees to ensure that employees do not compromise public confidence in our protection of tax account information in accordance with the Taxpayer Browsing Protection Act of 1997. The UNAX Program also tracks allegations of violations and works with the Human Capital Office, business program areas, and the Treasury Inspector General for Tax Administration (TIGTA) to investigate and take appropriate action, which can range from no finding of violation to termination and potential criminal charges. All IRS employees must receive the UNAX briefing and certify that they received the briefing annually. New employees must do the same within the first 30 days of their Entry on Duty (EOD) date or before being given access to taxpayer information, whichever is sooner. Seasonal employees and employees returning from extended leave, who did not certify to having received the briefing during the mandatory briefing period (May 2 - September 30 each year), must complete the UNAX briefing and certify that they received the briefing within the first 30 days of their Return to Duty date. Before being eligible to access any taxpayer information, an employee returning to duty after having a UNAX disciplinary action must complete the UNAX briefing and certify to having completed the briefing within 3 workdays of returning to duty.

The Safeguards Program provides oversight to external agencies in protecting federal taxpayer information and to internal customers in protecting taxpayer information,

employee information and other official use only information for contracting purposes. This office ensures that Federal, State and Local Agencies authorized to receive federal taxpayer information under various sections of Internal Revenue Code (IRC) Section 6103 are protecting the data in accordance with policy and legal requirements. On-site reviews are conducted at these Federal Agencies, State Welfare, Child Support, Revenue and local taxing authorities within a three-year cycle and reports issued to notify the agencies of any recommendations. In addition, Safeguard staff also conduct sensitive but unclassified contract document reviews for IRS contracts and acquisition documents to ensure that the legal and safeguards policy provisions are in place to protect taxpayer information.

Identity Theft

The IRS recognizes that taxpayers expect the IRS to safeguard personal information and provide timely resolution of identity theft related cases. To this end, about 18 months ago we began an aggressive strategy to research and address this growing problem. We established an Identity Theft Program Office charged with implementing the IRS' policy statement on identity theft. This Policy requires the IRS to take the necessary steps to provide assistance to victims of identity theft within the scope of their official duties.

Our Identity Theft Program Office works with offices throughout the IRS to implement the agencies' Identity Theft Enterprise Strategy comprised of three components—Outreach, Prevention and Victim Assistance. While the IRS took a number of immediate steps to address our strategy, we also recognized the importance of identifying and quantifying all of the material risks associated with identity theft at the agency.

As a result, in October 2005, we began a comprehensive Identity Theft Risk Assessment. Our analysis identified the potential for identity theft from both an external (impact to the IRS from an outside source) and internal (impact of an internal security breach) perspective. It also included a round table discussion with subject matter experts from financial institutions and fraud specialists to identity and leverage industry best practices and lessons learned. Working together we have developed remediation strategies which focus on encryption, enhancements of the IRS computer security and enhancing the current IRS computer security incident reporting system to specifically focus on identity theft Incident reporting, in order to better identify and track the disposition of identity theft incidents. While research shows that the IRS has one of the lowest instances of identity theft, we take this situation very seriously. We have made significant progress, but additional work remains---including implementing additional mediation strategies and conducting in-depth analyses of the remaining high-priority processes.

Being Proactive

One of the keys to protecting sensitive data is to be as proactive as possible. I have already referenced the review of our identity theft prevention procedures which we initiated 18 months ago.

In addition, as necessary, I personally notify business units with updates on security threats. For example, a year ago, I issued a memorandum in which I discussed information technology security guidance for the use of portable mass storage devices, such as flash disks, pen drives, key drives and thumb drives. These devices can be used to store a gigabyte of taxpayer information and other sensitive privacy information, but yet are so small as to make them more vulnerable to loss and theft.

I informed employees that if these devices are used to hold sensitive data that the data files must be encrypted using IRS approved encryption software. Furthermore, the devices should have no additional software/firmware beyond storage management and encryption. If an office has the need to use a portable mass storage device having an integrated central processing unit and other software applications, then it is subject to established security certification and accreditation processes.

We are also making an aggressive push for use of encryption solutions on all laptops. As discussed above, all users currently have the capability to encrypt all sensitive information. All of IRS's revenue agents have software that automatically encrypts the sensitive taxpayer information they might have.

One of the key initiatives that should serve to effectively mitigate the impact of any incidents of data loss involving IRS systems is the effort to field commercial security encryption solutions that will automatically encrypt all user data on IRS computers. We hope to have that fully deployed to all IRS laptop users within six months.

In addition, we have been proactive not only in the area of security but in our commitment to privacy as well. Almost one year ago, we took the initiative to implement OMB's directive to designate a Senior Agency Official for Privacy. Following the incident with the VA data loss, we have implemented OMB's directive to have our Senior Official for Privacy conduct a review of our policies and processes. This review will address all administrative, technical, and physical means used by IRS to control sensitive information, including but not limited to, procedures and restrictions on the use or removal of personally identifiable information beyond agency premises or control.

In addition, the Department of Homeland Security (DHS) and the Treasury Department have issued revised security incident reporting guidance and are working on implementing that revised guidance.

In terms of the reporting of loss or theft of IRS equipment or data, we are in a somewhat unique position. TIGTA provides independent oversight of IRS activities by conducting audits and investigations involving IRS programs and operations If an employee loses any IT equipment, as happened in the recent instance, he/she must report it to his manager who shall insure that the incident is reported to the Computer Security Incident Response Capability (CSIRC) and to TIGTA. These incidents are also reported to the Department of the Treasury and through Treasury to the Department of Homeland Security as appropriate. The report must include whether the sensitive data is encrypted. For incidents involving the potential loss of employee information, taxpayer information,

or other sensitive information, follow-up reports are made by the manager until the incident is resolved by TIGTA or the IRS.

Conclusions

Mr. Chairman, in conclusion, I would like to emphasize the following points:

- Privacy and information security are a growing concern in virtually every organization, both public and private;
- As technology advances, our ability to protect sensitive information must advance as well to meet new threats;
- The IRS is committed to the highest standards of protection for both sensitive taxpayer data as well as personally identifiable information;
- We have in place a robust program that focuses on security in information technology and privacy;
- We have adopted the layered “defense in depth” approach to our security defenses forcing any attacker to defeat multiple layers of security to get to our data.
- We believe the expanded use of automated encryption solutions will be a major technical component of our comprehensive strategy to effectively counter the threats posed by potential data losses
- We have attempted to be proactive in addressing potential security threats;
- We are complying fully with recent directives issued by OMB to review our policies and procedures to ensure the IRS has adequate safeguards to prevent the misuse or unauthorized access to personally identifiable information;
- In the event an incident occurs where equipment of data is lost, we refer the matter to TIGTA for investigation;
- Our biggest challenges seem to be more in the effective implementation of existing security and privacy policies and processes, and training the staff to make use of security tools and capabilities that already exist on IRS computers: and
- Despite all of our progress that we have made, as TIGTA reminds us in their audits, we continue to have significant work to do.

I appreciate the opportunity to appear and I will be happy to respond to any questions.